(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 57 697 A 1**

(51) Int. Cl.[7]: G 06 F 12/14

(21) Aktenzeichen: 100 57 697.4
(22) Anmeldetag: 21. 11. 2000
(43) Offenlegungstag: 29. 5. 2002

DE 100 57 697 A 1

(71) Anmelder:
Fujitsu Siemens Computers GmbH, 81739 München, DE

(74) Vertreter:
Epping, Hermann & Fischer, 80339 München

(72) Erfinder:
Schnitzmeier, Werner, 86343 Königsbrunn, DE

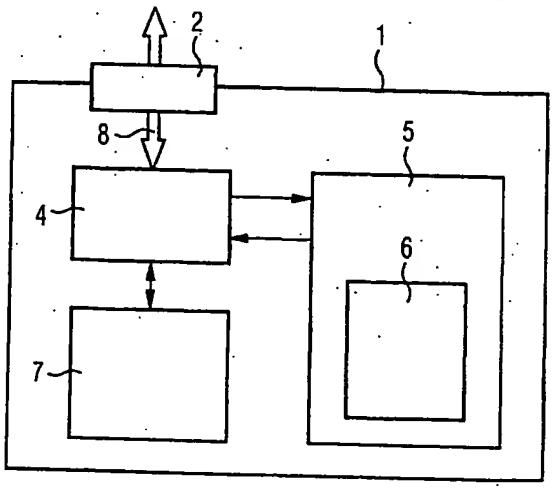
(56) Entgegenhaltungen:
DE 195 45 020 A1
JP 2000076443 A (abstract) World Patent Index (online) Derwent (recherchiert am 13.06.01), In: STN, Accession No. 2000-2782 65 (24) WPIDS;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Speichermedium

(57) Die Erfindung betrifft ein Speichermedium mit einer Speichereinheit (7) und einer Authentifizierungseinheit (5) mit einem Fingerprintsensor (6). Der Zugriff auf das Speichermedium erfolgt über eine USB-Schnittstelle (2). Der Lese- und/oder Schreibzugriff auf den Inhalt der Speichereinheit (7) ist gesperrt und die Sperre nur durch die Authentifizierung eines Benutzers über den Fingerprintsensor (6) aufhebbar.



DE 100 57 697 A 1

Beschreibung

[0001] Die Erfindung betrifft ein Speichermedium, das insbesondere zum mobilen Einsatz geeignet ist.

[0002] Mobile Speichermedien sind in einer großen Vielzahl bekannt. Für kleine Datenmengen sind beispielsweise Disketten üblich. Bei größeren Datenmengen werden oftmals die sogenannten ZIP-Datenträger der Firma Iomega oder Wechselplatten verwendet. Außerdem sind Flash-Speicher im Einsatz. Neben Problemen wie kleiner Speicherkapazität (Disketten) oder der Erfordernis eines speziellen Laufwerks (ZIP-Datenträger) ist oftmals der Schutz vor einem unberechtigten Zugriff unbefriedigend. Zwar besteht die Möglichkeit, die Inhalte der oben genannten Speichermedien durch ein Paßwort zu schützen, allerdings ist dieser Schutz in der Regel mit verhältnismäßig kleinem Aufwand überwindbar.

[0003] Aufgabe der Erfindung ist es daher, ein Speichermedium anzugeben, das einen verbesserten Schutz vor unberechtigtem Zugriff bietet.

[0004] Diese Aufgabe wird durch ein Speichermedium mit einer Speichereinheit, einer USB-Schnittstelle zum Zugriff auf den Inhalt der Speichereinheit und einer Authentifizierungseinheit mit einem Fingerprintsensor zur Authentifizierung eines Benutzers gelöst, wobei der Lese- und/oder Schreibzugriff auf den Speicherinhalt gesperrt ist und die Sperre durch die Authentifizierung eines Benutzers über den Fingerprintsensor aufhebbar ist.

[0005] Die Aufgabe wird außerdem durch ein Speichermedium gelöst mit einer Speichereinheit, einer USB-Schnittstelle zum Zugriff auf den Inhalt der Speichereinheit und einer Authentifizierungseinheit mit einem Fingerprintsensor zur Authentifizierung eines Benutzers, wobei Daten in der Speichereinheit verschlüsselt ablegbar sind und zur Entschlüsselung die Authentifizierung des Benutzers über den Fingerprintsensor erforderlich ist.

[0006] In dem erfindungsgemäßen Speichermedium abgelegte Daten können also auf zweierlei Weise geschützt werden. Zum einen ist es möglich, einfach den Lese- und/oder Schreibzugriff so lange zu verhindern, bis ein berechtigter Benutzer authentifiziert ist. Andererseits ist es auch möglich, die Daten zu verschlüsseln und eine Entschlüsselung nur nach Authentifizierung eines berechtigten Benutzers zuzulassen. Zur Erzielung eines besonders guten Schutzes können beide Schutzkonzepte kombiniert werden.

[0007] Im erstgenannten Fall wird also nur der gesperrte Zugriff freigegeben. Auf regulärem Weg ist es daher nicht mehr möglich, an die gespeicherten Daten zu gelangen. Durch Eingriff in das Speichermedium selber bleibt aber die Möglichkeit, unberechtigterweise Kenntnis von den gespeicherten Daten zu erhalten. In der zweitgenannten Möglichkeit ist dies auch verhindert, da die Daten selber verschlüsselt abgelegt werden. Allerdings ist sowohl beim Schreiben als auch beim Lesen eine Verschlüsselung der Daten notwendig, was die Zugriffsgeschwindigkeit verlangsamt.

[0008] Besonders vorteilhaft ist die Ausgestaltung der Schnittstelle nach dem USB-Standard. Dadurch ist es möglich, das Speichermedium bei laufendem Betrieb eines Computersystems an dieses anzuschließen beziehungsweise von diesem zu trennen. Das Speichermedium wird dann bei Verwendung eines geeigneten Betriebssystems automatisch erkannt und steht beispielsweise als zusätzliches Laufwerk zur Verfügung.

[0009] Bei der Identifizierung des Speichermediums erfolgt dann eine automatische Abfrage der Zugriffsrechte. Nach der Authentifizierung des Benutzers durch Auflegen des Fingers auf den Fingerprintsensor kann der Zugriff auf den Inhalt des Speichermediums erfolgen.

[0010] Die Erfindung wird nachfolgend anhand eines Ausführungsbeispieles näher erläutert. Es zeigt:

[0011] Fig. 1 den schematischen Aufbau eines erfindungsgemäßen Speichermediums und

[0012] Fig. 2 eine dreidimensionale Darstellung eines erfindungsgemäßen Speichermediums.

[0013] In Fig. 1 ist ein erfindungsgemäßes Speichermedium 1 als Blockschaltbild dargestellt. Über eine USB-Schnittstelle 2 wird das Speichermedium an ein beliebiges anderes Gerät mit USB-Schnittstelle angeschlossen. Von dort aus erfolgt der Zugriff auf das Speichermedium. Beispielsweise sollen Daten aus dem Speichermedium ausgelesen werden. Eine solche Leseanfrage wird zunächst an eine Zugriffsüberwachungseinheit 4 geleitet. Falls der Zugriff auf eine Speichereinheit bereits bei einem früheren Lese- oder Schreibvorgang freigegeben wurde, kann sofort auf die Speichereinheit 7 zugegriffen werden.

[0014] Falls es sich aber um den ersten Zugriff handelt, wird der Zugriff auf den Speicherinhalt so lange verweigert, bis über eine Authentifizierungseinheit 5 mit einem Fingerprintsensor 6 ermittelt wurde, ob eine Berechtigung vorliegt. Dazu ist die Zugriffsüberwachungseinheit 4 mit der Authentifizierungseinheit 5 verbunden. Der Benutzer legt seinen Finger auf den Fingerprintsensor 6 auf, so daß der Fingerabdruck gelesen werden kann. Anschließend analysiert die Authentifizierungseinheit 5 den Fingerabdruck und identifiziert charakteristische Linien, sogenannte Minutien. In der Regel genügen zwanzig bis dreißig Minutien, um eine zuverlässige Erkennung zu gewährleisten. Die Minutien werden mit in einem Speicher der Authentifizierungseinheit 5 abgelegten Benutzerdaten verglichen. Wenn die Prüfung ergibt, daß der Benutzer zum Zugriff auf das Speichermedium berechtigt ist, wird ein dies anzeigendes Signal an die Zugriffsüberwachungseinheit 4 zurückgegeben.

[0015] Um eine möglichst kleine Bauform zu erreichen ist, es auch möglich, statt eines Fingerprintsensors 6, der den gesamten Fingerabdruck lesen kann, einen Streifensensor zu verwenden. In diesem Fall würde der Finger nicht aufgelegt werden, sondern müßte über den Streifensensor bewegt werden.

[0016] Nach Freigabe des Zugriffs durch die Zugriffsüberwachungseinheit 4 kann nun beliebig auf den Speicherinhalt über die USB-Schnittstelle 2 zugegriffen werden. Zusätzlich können für verschiedene Benutzer verschiedene Zugriffsrechte vergeben werden, beispielsweise nur ein Lesezugriff oder nur ein Schreibzugriff oder nur ein Zugriff auf bestimmte Speicherbereiche.

[0017] Wenn das Speichermedium so ausgestaltet ist, daß die Daten verschlüsselt in der Speichereinheit 7 abgelegt sind, übernimmt die Zugriffsüberwachungseinheit 4 ebenfalls die Funktion des Ver- und Entschlüsselns. Die Zugriffsüberwachungseinheit 4 ist in Fig. 1 als separater Block dargestellt. Sie kann natürlich ebenso als Teil der Authentifizierungseinheit 5 realisiert werden.

[0018] In der Fig. 2 ist das Speichermedium, dessen Funktion anhand der Fig. 1 beschrieben wurde, als Gerät dargestellt. Das Gerät ist im wesentlichen quaderförmig. An einer Stirnfläche 12 ist ein Stecker 11 der USB-Schnittstelle 2 dargestellt. Auf einer Seitenfläche 13 ist der Fingerprintsensor 6 angeordnet. An dem steckerseitigen Ende der Seitenfläche 13 ist eine Abschrägung als Griffffläche 14 vorgesehen. Dadurch kann das Speichermedium gut aus einem USB-Gegenstecker wieder herausgezogen werden.

[0019] Zur Benutzung eines erfindungsgemäßen Speichermediums wird das Speichermedium an die USB-Schnittstelle eines beliebigen Gerätes angeschlossen. Wenn dies ein Computer ist mit einem den USB-Standard unterstützenden Betriebssystem, so wird das Speichermedium

automatisch als zusätzliches Laufwerk erkannt. Der Zugriff erfolgt dann wie auf ein normales Festplattenlaufwerk oder beispielsweise auf eine Diskette.

Bezugszeichenliste

1 Speichermedium
2 USB-Schnittstelle
4 Zugriffsüberwachungseinheit
5 Authentifizierungseinheit
6 Fingerprintsensor
7 Speichereinheit
11 USB-Stecker
12 Stirnfläche
13 Seitenfläche
14 Griffläche

Patentansprüche

1. Speichermedium mit
einer Speichereinheit (7),
einer USB-Schnittstelle (2) zum Zugriff auf den Inhalt der Speichereinheit (7) und
einer Authentifizierungseinheit (5) mit einem Fingerprintsensor (6) zur Authentifizierung eines Benutzers,
wobei der Lese- und/oder Schreibzugriff auf die Speichereinheit (7) gesperrt ist und die Sperre durch die Authentifizierung eines Benutzers über den Fingerprintsensor (6) aufhebbar ist.

2. Speichermedium mit
einer Speichereinheit (7),
einer USB-Schnittstelle (2) zum Zugriff auf den Inhalt der Speichereinheit (7) und
einer Authentifizierungseinheit (5) mit einem Fingerprintsensor (6) zur Authentifizierung eines Benutzers,
wobei Daten in der Speichereinheit (7) verschlüsselt ablegbar sind und zur Entschlüsselung die Authentifizierung des Benutzers erforderlich ist.

3. Speichermedium nach Anspruch 2, dadurch gekennzeichnet, daß der Zugriff auf den Schlüssel gesperrt ist und die Sperre durch die Authentifizierung eines Benutzers über den Fingerprintsensor (6) aufhebbar ist.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 100 57 697 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 29. Mai 2002

FIG 1

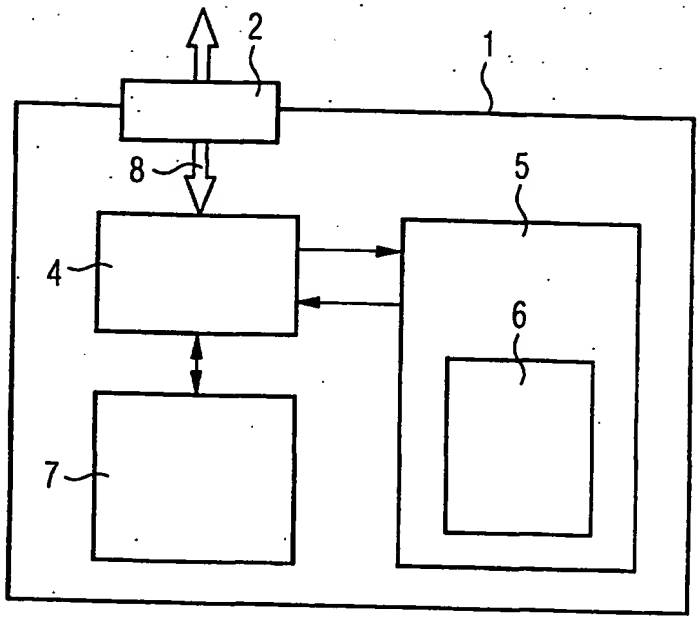


FIG 2